PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 : H04L 9/14, 9/30, H04N 7/16 — A1

(11) International Publication Number: WO 91/12680

(43) International Publication Date: 22 August 1991 (22.08.91)

(21) International Application Number: PCT/GB91/00227

(22) International Filing Date: 14 February 1991 (14.02.91)

(30) Priority data:
9003326.7 14 February 1990 (14.02.90) GB

(71) Applicant *(for all designated States except US)*: ENFRANCHISE SIXTY LIMITED [GB/GB]; St John's Innovation Centre, Cowley Road, Cambridge CB4 4WS (GB).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)* : HAWTHORNE, William, McMullan [GB/GB]; Kenmare, Bramerton Road, Surlingham, Norfolk, Norwich NR14 7DE (GB).

(74) Agent: JONES, William; Willow Lane House, Willow Lane, Norwich, Norfolk NR1 2EU (GB).

(81) Designated States: AT, AT (European patent), AU, BB, BE (European patent), BF (OAPI patent), BG, BJ (OAPI patent), BR, CA, CF (OAPI patent), CG (OAPI patent), CH, CH (European patent), CM (OAPI patent), DE, DE (European patent), DK, DK (European patent), ES, ES (European patent), FI, FR (European patent), GA (OAPI patent), GB, GB (European patent), GR (European patent), HU, IT (European patent), JP, KP, KR, LK, LU, LU (European patent), MC, MG, ML (OAPI patent), MR (OAPI patent), MW, NL, NL (European patent), NO, PL, RO, SD, SE, SE (European patent), SN (OAPI patent), SU, TD (OAPI patent), TG (OAPI patent), US.

Published
With international search report.

(54) Title: APPARATUS AND METHOD FOR DATA COMMUNICATION

(57) Abstract

A method of communicating data from a first transmitting station to a selected second receiving station in a network of stations adapted for communication with one another, said method comprising: locally storing a substantially unique key at each station, all the keys being known to users at all the stations; locally storing a common key symmetric message ciphering first algorithm at each station; generating at the first station a working key as a predetermined representation of the unique key which identifies the intended recipient station; ciphering the data to be transmitted by use of said working key in said first algorithm; and transmitting said ciphered data, whereby to permit deciphering of said ciphered data by the selected second station. An apparatus, and network, for this method are also disclosed.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	ES	Spain	MG	Madagascar
AU	Australia	FI	Finland	ML	Mali
BB	Barbados	FR	France	MN	Mongolia
BE	Belgium	GA	Gabon	MR	Mauritania
BF	Burkina Faso	GB	United Kingdom	MW	Malawi
BG	Bulgaria	GN	Guinea	NL	Netherlands
BJ	Benin	GR	Greece	NO	Norway
BR	Brazil	HU	Hungary	PL	Poland
CA	Canada	IT	Italy	RO	Romania
CF	Central African Republic	JP	Japan	SD	Sudan
CG	Congo	KP	Democratic People's Republic of Korea	SE	Sweden
CH	Switzerland			SN	Senegal
CI	Côte d'Ivoire	KR	Republic of Korea	SU	Soviet Union
CM	Cameroon	LI	Liechtenstein	TD	Chad
CS	Czechoslovakia	LK	Sri Lanka	TG	Togo
DE	Germany	LU	Luxembourg	US	United States of America
DK	Denmark	MC	Monaco		

APPARATUS AND METHOD FOR DATA COMMUNICATION

Field of the Invention

This invention relates to the communication of data between stations in a network of stations adapted for communication with one another. The invention is applicable primarily to digital electronic communication, for example the transmission of messages between facsimile transceivers, the transmission of data between computers, electronic mail, and digital telephony. The data can be any data for example computer data, the content of a message to be sent by fax (i.e facsimile) or by electronic mail, or the content of a telephone conversation.

Background to the Invention

It is often desired to transmit private or confidential data. In a network of spaced-apart stations the communication lines between the stations may well be accessible to third parties, e.g hackers or tappers. With fax machines it is quite easy to send messages accidentally to the wrong destination. These problems become greater as the network becomes more extensive, for example the public telephone system. There is therefore an existing need for a reliable means of enciphering data transmissions to make it difficult for hackers and other unintended recipients to extract the original data from an enciphered data transmission.

Certain solutions to this problem are currently available, but many of these existing solutions fail to meet desired criteria at one or other point. Ordinarily desired criteria are a reasonably low cost

and a low level of administration coupled with a high level of difficulty for an unintended recipient to decipher a ciphered transmission. Different users attach different priorities to these criteria. For example some commercial data and electronic fund transfer transactions among banks and between banks and their customers constitute valuable and confidential data, and in that case the level of difficulty presented to an unintended recipient must be such as to make it seriously uneconomic or unrealistically time-consuming to attempt to decipher the ciphered data.

A further consideration is whether or not enciphering and deciphering are to take place on the fly, i.e the plain message is enciphered at the output of the transmitter and deciphered at the input of the receiver. An alternative is to encipher a message and hold it on file, e.g in a computer memory, prior to transmission. The enciphered message can then be sent by modem or other means without adaptation to the technology of the communication channel between the stations. The received ciphered message can be stored in the receiver's computer memory and deciphered at a later time. It is usually convenient to encipher and decipher on the fly and this is obviously a necessary criterion for digital telephony applications.

One presently used solution is to provide each station in the network with secret information concerning which cipher key is to be used for ciphering data to be transmitted between each pair of stations. This information has to be agreed and distributed in advance and kept secret, and therefore the administrative problems in a network of any size are formidable and the likelihood of loss of security is considerable. The information needs to be changed from time to time or after any leakage, adding to the administrative problems. It will be appreciated that if all the stations agree to use a common key then all users can read all the data and one security lapse opens the entire network. If each pair of transmitters and receivers in a network of N stations wish to preserve mutual secrecy, the number of keys

required is N x (N-1)/2, i.e 4950 different keys for a network of 100 stations. If different keys are required for a message from A to B and a message from B to A then the number of keys required is N x (N-1), i.e 9900 different keys for a network of 100 stations.

Another existing proposal in the art is to replace the supposedly secret keys with public keys, and instead to require a prior separate communication from A to B to enable both A and B to generate an agreed secret key specific to the occasion of transmitting a particular enciphered data message. The separate communication poses problems both administratively and as to potential loss of security.

An object of the present invention is to provide an apparatus and method which takes into account the desired criteria and which mitigates the described disadvantages.

Summary of the Invention

According to the present invention there is provided a method of communicating data from a first transmitting station to a selected second receiving station in a network of stations adapted for communication with one another, characterised by said method comprising:

locally storing a substantially unique key at each station, all the keys being known to users at all the stations;

locally storing a common key symmetric message ciphering first algorithm at each station;

generating at the first station a working key as a predetermined representation of the unique key which identifies the intended recipient station;

ciphering the data to be transmitted by use of said working key in said first algorithm; and

transmitting said ciphered data, whereby to permit deciphering of said ciphered data by the selected second station.

This method can be used for example for fax transmissions or digital telephony where the routine requirement for confidentiality is relatively low.

According to the invention in another aspect there is provided a method of communicating data according to the aforementioned method characterised by said method also comprising:

locally storing a common ciphering second algorithm at each station;

generating at the first station a transmission initiation request as a combination of the unique keys which identify respectively the first station and the selected second station intended to receive a data transmission from the first station; and

ciphering said request by use of said second algorithm, whereby the ciphered request constitutes the working key.

The invention further provides a method of gaining access to the data transmitted in enciphered form by communication method as disclosed in the immediately preceding paragraph, said method comprising:

locally generating, at a station actually receiving the transmission signal, a working key by ciphering with said second algorithm a combination of the known unique keys which identify respectively the transmitting station and the local receiving station; and

applying said first algorithm using said locally generated working key to said received transmission signal, whereby said transmission is deciphered to recreate said data only if said local receiving station has the substantially unique key identifying the intended recipient station and can thereby locally generate a working key identical to the working key used at the transmitting station.

In another aspect of the communication method, each station also locally stores a substantially unique membership key, all the membership keys being known to users at all the stations; and

said transmission initiation request is generated as a combination of the unique station key and the unique membership key of the first station together with the unique station key and the unique membership key of the intended recipient station.

In this embodiment a station actually receiving a transmission signal can decipher the transmission to recreate the data only if said receiving station has both the unique station key and the unique membership key identifying the intended recipient station.

In yet another aspect of the communication method, a common key symmetric ciphering third algorithm is locally stored at each station; a substantially random key is enciphered by used of said working key and said third algorithm; said data to be transmitted is ciphered by use of said random key in said first algorithm; and said ciphered random key is transmitted together with the ciphered data as said transmission signal, whereby to permit local deciphering of the enciphered random key and consequently of the ciphered data substantially only by an intended recipient station.

The third algorithm may be identical to the first algorithm.

The methods disclosed in the above paragraphs within this section permit the enforcement of successively higher levels of security and can be used for example for transmission of valuable or confidential data between main frame computers.

The invention also provides, separately, the transmission and reception methods embodied in the communication methods disclosed above.

The invention further provides a communication network for carrying out the communication methods described above as well as, separately, transmission and reception apparatus embodied in the communication network, and transceiver apparatus selectively operable in transmission or reception modes embodied in the communication network.

The invention further provides apparatus for use with any such communication apparatus to enable the communication apparatus to carry out the disclosed methods.

Yet further, the invention provides a method, and separately an apparatus, for communicating data substantially as described herein; and in certain embodiments with reference to, and as illustrated in, the accompanying drawings.

Embodiments of the invention will now be described, by way of example, with reference to the drawings that follow; in which:

Brief Description of the Drawings

Figure 1 is a flow chart summarising the operation of the third and fourth embodiments of the present invention in the transmission mode; and

Figure 2 is a flow chart summarising operation of the third and fourth embodiments of the present invention in the reception mode.

Description of the Preferred Embodiments

The first embodiment is applicable e.g to fax transmissions, and also to electronic mail and digital telephony, where the routine requirement for confidentiality is relatively low. For fax, the ordinary requirement is to ensure that if the destination telephone number for a fax message is incorrectly dialled and the transmission is therefore received at the wrong receiver, the message is unintelligible at that wrong receiver. The first embodiment can solve this problem of protection from dialling errors.

Each fax transceiver in the network is provided with a tamper-proof control means such as a sealed box, board or integrated circuit connected to or embedded within the transceiver. The control means is selectively operable in transmission and reception modes and comprises a memory for storing a key and an algorithm, processing means for running the algorithm, means for reading a fax number and means, such as a keypad, allowing entry of a key such as a number or number and letter combination. If this embodiment is utilised by an original equipment manufacturer, the control means can be incorporated into the design of the fax transceiver, in which case the telephone/fax dialling keys can themselves serve the additional function of allowing entry of the key number.

The memory in each control means stores a key which is unique to that control means and which is suitably read from the transceiver as its own public telephone/fax number. This unique key is thus a public key and is known to users at all the stations. The memory in each control means also stores a common key symmetric message ciphering first algorithm. A key symmetric

algorithm is a cipher which, in response to activation by a key, converts an intelligible stream of letters and numbers, i.e the message, into an unintelligible stream, and which also operates in reverse to convert the unintelligible stream back to the intelligible stream upon activation by an identical key.

When a user at a first fax transceiver wishes to send a message he dials or keys in the public fax number of the intended recipient to make a line connection. The control means also reads this number and takes the last four digits as a working key. When the two stations are connected and have completed their introduction protocol and checked the line quality, the message is transmitted via the processor in the control means. The processor operates to cipher the data on the fly by use of the working key in the first algorithm. The recipient station can similarly use its control means to decipher the received data on the fly by use of the identical working key in its own stored first algorithm. The recipient's working key is identical because it is the last four digits of the recipient's own public fax number and is available in the control means in reception mode.

Generally, in order to protect transmissions more strictly against dialling errors or interception, each station in the network which subscribes to an organised message ciphering facility is preferably also provided with a substantially unique membership key. The key may be valid for an indefinite term or for a fixed period against a charge, and then changed. The working key is then formed as the last four digits of the intended recipient's fax number together with the four digits of the intended recipient's membership key. The keypad allows entry of the intended recipient's membership key into the memory of the control means. The processor operates as before to encipher the data on the fly by use of the 8-digit working key in the first algorithm. Any dialling error will then result in the message being enciphered by use of a working key created from a combination of fax number

and membership key number which does not exist and therefore no recipient can decipher the ciphered transmission.

The second embodiment is similar in principle to the first embodiment and is applicable to digital telephony. Each telephone handset is provided with a similar control means to the first embodiment except that, for telephony, the control means is adapted to operate simultaneously in send and receive modes and is adapted to switch from an inactive to an active state upon reception of data to be received and data to be transmitted. The control means is preferably embodied in an integrated circuit contained within the telephone handset, and the telephone keypad then also serves to enter the keys required to initiate enciphering of a telephone conversation.

The working key is formed as a combination of the call originator's unique public key (e.g the last portion of his telephone number) and his unique membership key together with the unique key and the unique membership key of the intended recipient. The unique keys and the unique membership keys are all known to all subscribers to the telephone ciphering facility, and it will be appreciated that each unique key is associated with a specific unique membership key. The working key may then be used as described above in the stored first algorithm to encipher the call originator's conversation, or other data he may wish to transmit over the telephone channel, on the fly. The correct intended recipient station can likewise decipher the transmitted enciphered conversation on the fly and can respond. It will be appreciated that the working key formed at the responding station for use in creating a responding enciphered conversation is different from the call originator's working key because the four keys used to create the working key are combined in a different succession. Thus the working key used for transmissions from A to B differs from the working key used for transmissions from B to A.

The third and fourth embodiments will now be described with reference to Figures 1 and 2; these Figures may be understood using the identification table that follows:

IDENTIFICATION TABLE

Figure 1

1	Input receiver's station public key.
2	Input receiver's membership key.
3	Input any additional agreed key.
4	Generate transmission initiation request.
5	Use second algorithm and transmission initiation request to generate working key.
6	Generate random key (if used).
7	Use third algorithm and working key to encipher the random key.
8	Transmit enciphered random key.
9	Use first (message) algorithm and either the working key or the random key to encipher the message.
10	Transmit the enciphered message.

Figure 2

11	Input transmitter's station public key.

12 Input transmitter's membership key.

13 Input any additional agreed key.

14 Generate the transmission initiation request.

15 Use the second algorithm and the transmission initiation request to generate the working key.

16 Input the received enciphered random key (if used).

17 Use the third algorithm and the working key to decipher the random key.

18 Use the first (message) algorithm and either the working key or the random key to decipher the received message.

The third embodiment is applicable e.g to digital telephony electronic mail or data transmission between computers, for example, where a higher level of security is required. In this embodiment the working key is not simply a combination of the keys as described above, but is an enciphered version thereof. Each control means of each telephone or station in the network is further provided with a locally stored common ciphering second algorithm.

When a conversation, or other data transmission (see Figure 1), is required the call originator generates a transmission initiation request comprising a combination of the unique keys which identify respectively the call originator's telephone and the intended recipient's telephone and preferably also together with unique membership keys of the call originator and of the intended recipient. The transmission initiation request is then enciphered by use of the second algorithm whereby the enciphered request

constitutes the working key. The working key is then used in the first algorithm to encipher the data on the fly as before.

It will be appreciated that yet a further key can be added to the combination used in forming the working key in any of the above described embodiments. The further key may be regarded as an addition to the membership key. The further key would be for example a number known only to a selected group of persons from among those who might be users of the receiving fax or telephone apparatus. The receiving station (see Figure 2) would then only operate to decipher the incoming enciphered message if a person from the selected group had previously attended and keyed in the further key. The further key must have been agreed between transmitter and receiver in a previous communication of any kind. In the case of a fax message the received enciphered message can be held in computer memory in ciphered form until the authorised person with the further agreed key is available.

The fourth embodiment is applicable to communication between main frame digital computers, for example, where a very high level of security is required. In this embodiment a working key is formed as described in relation to the third embodiment. A random number generator is operated to provide a random number. The random number is then itself enciphered by using the working key in a third algorithm to produce a ciphered random key. The third algorithm is a common key symmetric algorithm and is locally stored at each station. The third algorithm may be the same as the first algorithm. The data to be transmitted is then enciphered by use of the random key in the first algorithm and the ciphered random key is itself transmitted together with the transmitted ciphered data (see Figure 1).

The intended recipient station locally generates its own working key and deciphers the transmitted ciphered random key by use of the working key in the locally stored third algorithm. The random

key is then available for use in deciphering the transmitted ciphered data (see Figure 2).

In all the described embodiments the data to be transmitted is enciphered by use of a key in the first algorithm. The key is of sufficient length as to be capable of producing a large number of variants, preferably greater than 1×10^{16}.

The working key is, in the higher security embodiments, produced by enciphering a combination of inputted keys by means of a second algorithm. The second algorithm is preferably a fixed key transformation algorithm, the fixed key being chosen from a very large number of possible variants, preferably greater than 1×10^{30}. The second algorithm is not a key symmetric algorithm since reversibility is not required. Each station has the available information to produce the necessary working key when required and when called by a station desiring to transmit data thereto. The second algorithm thus requires a one-way transformation only and can accordingly be selected by those skilled in the art to be sufficiently difficult as to make it seriously uneconomic or unrealistically time-consuming to attempt to decipher the captured data.

CLAIMS:

1. A method of communicating data from a first transmitting station to a selected second receiving station in a network of stations adapted for communication with one another, said method comprising:

locally storing a substantially unique key at each station, all the keys being known to users at all the stations;

locally storing a common key symmetric message ciphering first algorithm at each station;

generating at the first station a working key as a predetermined representation of the unique key which identifies the intended recipient station;

ciphering the data to be transmitted by use of said working key in said first algorithm; and

transmitting said ciphered data, whereby to permit deciphering of said ciphered data by the selected second station.

2. A method of communicating data according to Claim 1, characterised by said method also comprising:

locally storing a common ciphering second algorithm at each station;

generating at the first station a transmission initiation request as a combination of the unique keys which identify respectively the first station and the selected second station intended to receive a data transmission from the first station;

ciphering said request by use of said second algorithm, whereby the ciphered request constitutes the working key.

3. A method of communicating data according to Claim 2, characterised in that each station also locally stores a substantially unique membership key, all the membership keys being known to users at all the stations; and

said transmission initiation request is generated as a combination of the unique station key and the unique membership key of the first station together with the unique station key and the unique membership key of the intended recipient station.

4. A method of communicating data according to Claim 2 or Claim 3, characterised in that a common key symmetric ciphering third algorithm is locally stored at each station; a substantially random key is enciphered by use of said working key and said third algorithm; said data to be transmitted is ciphered by use of said random key in said first algorithm; and said ciphered random key is transmitted together with the ciphered data as said transmission signal, whereby to permit local deciphering of the enciphered random key and consequently of the ciphered data substantially only by an intended recipient station.

5. A method of communicating data according to Claim 4, characterised in that the third algorithm is identical to the first algorithm.

6. A method of gaining access to the data transmitted in enciphered form by communication method according to Claim 2, characterised by said method comprising:

locally generating, at a station actually receiving the transmission signal, a working key by ciphering with said second algorithm a combination of the known unique keys which identify respectively the transmitting station and the local receiving station; and

applying said first algorithm using said locally generated working key to said received transmission signal, whereby said transmission is deciphered to recreate said data only if said local receiving station has the substantially unique key identifying the intended recipient station and can thereby locally generate a working key identical to the working key used at the transmitting station.

7. A method of gaining access to the data transmitted in enciphered form by a communication method according to Claim 3, characterised by said method comprising:

locally generating, at a station actually receiving the transmission signal, a working key by ciphering with said second algorithm a combination of the known unique keys, which identify respectively the transmitting station and the local receiving station, and the known unique membership keys identifying respectively the transmitting station and the local receiving station; and

applying said first algorithm using said locally generated working key to said received transmission signal, whereby said transmission is deciphered to recreate said data only if said local receiving station has the substantially unique key identifying the intended recipient station and the substantially unique membership key of the intended recipient station, and can thereby locally generate a working key identical to the working key used at the transmitting station.

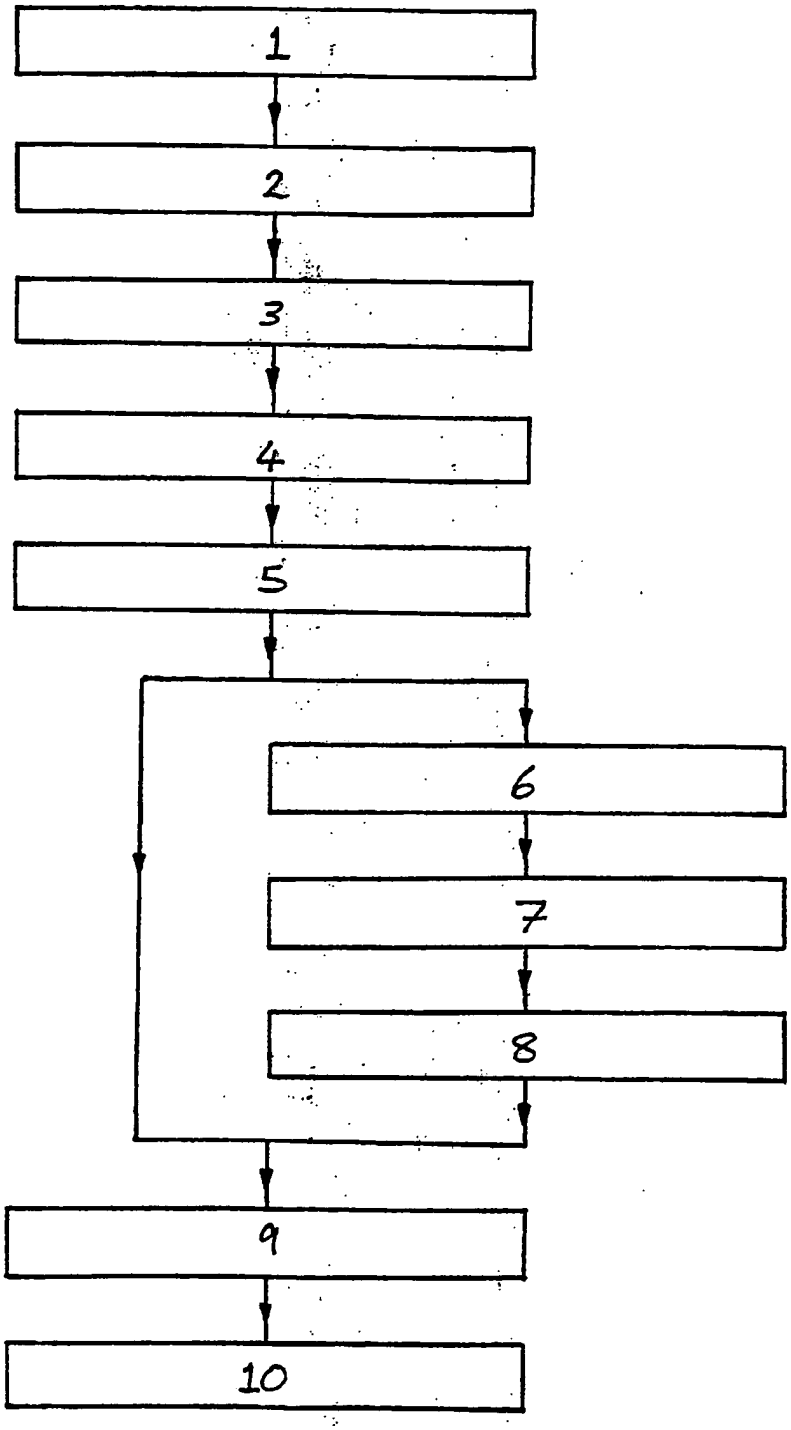
8. A data transmission apparatus, characterised in that the apparatus is suitable for carrying out the communication methods according to any one of Claims 1 to 5.

9. A data reception apparatus, characterised in that the apparatus is suitable for carrying out the communication methods according to any one of Claims 1 to 5.

10. A communication network characterised in that the network is suitable for carrying out the communication methods according to any one of Claims 1 to 5.

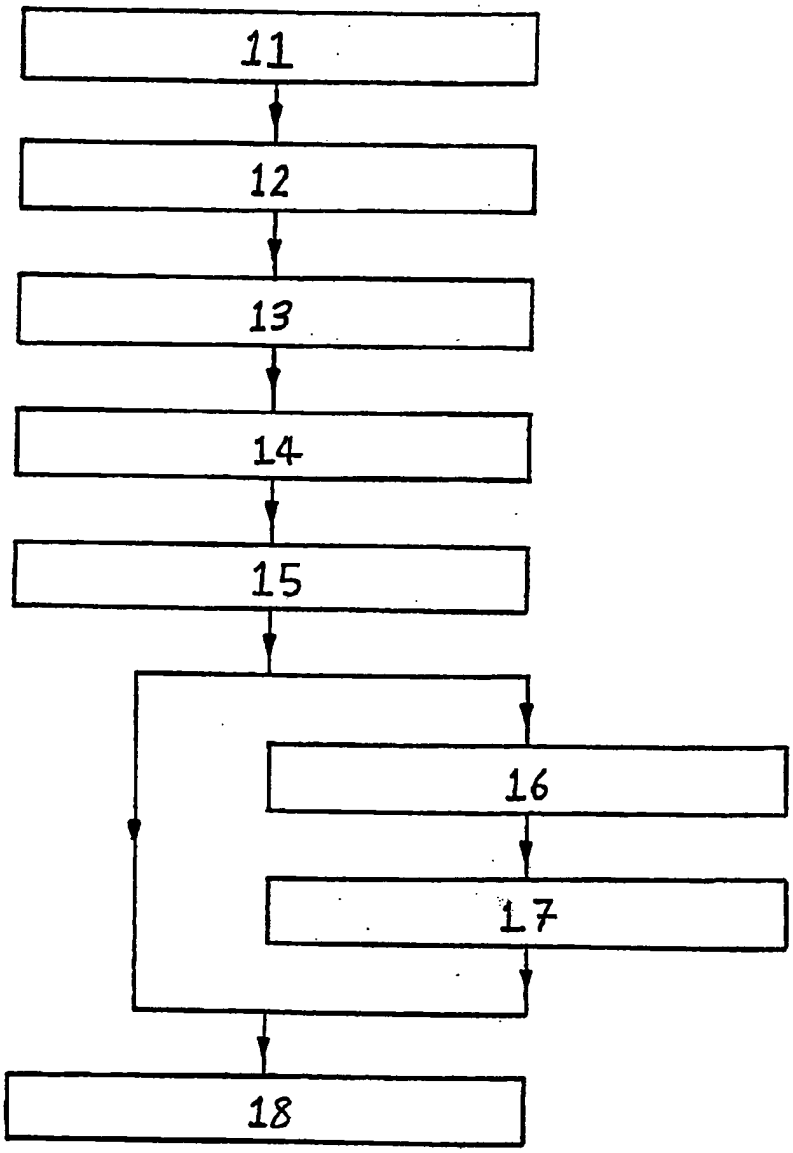
1/2

FIGURE 1



2/2

FIGURE 2



INTERNATIONAL SEARCH REPORT

International Application No PCT/GB 91/00227

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) [6]

According to International Patent Classification (IPC) or to both National Classification and IPC

IPC[5]: H 04 L 9/14,H 04 L 9/30,H 04 N 7/16

II. FIELDS SEARCHED

Minimum Documentation Searched [7]

Classification System	Classification Symbols
IPC[5]	H 04 L,H 04 N

Documentation Searched other than Minimum Documentation to the Extent that such Documents are included in the Fields Searched [8]

III. DOCUMENTS CONSIDERED TO BE RELEVANT [9]

Category [10]	Citation of Document, [11] with indication, where appropriate, of the relevant passages [12]	Relevant to Claim No. [13]
A	EP, A1, 0 127 381 (M/A-COM LINKABIT) 05 December 1984 (05.12.84), see abstract; page 1, line 20 - page 6, line 11. --	1
A	US, A, 4 887 296 (HORNE) 12 December 1989 (12.12.89), see abstract; column 4, lines 28-44; column 6, lines 38-65; fig. 1. --	1
A	EP, A1, 0 287 720 (INTERNATIONAL BUSINNES MACHINES) 26 October 1988 (26.10.88), see abstract; claim 1. --	1
A	EP, A1, 0 123 360 (N.V. PHILIPS'GLOEILAMPEN-FABRIKEN) 31 October 1984	1

* Special categories of cited documents: [10]

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report
10 May 1991	28. 05. 91
International Searching Authority	**Signature of Authorized Officer**
EUROPEAN PATENT OFFICE	M. PEIS M. Peis

Form PCT/ISA/210 (second sheet) (January 1985)

III. DOCUMENTS CONSIDERED TO BE RELEVANT (CONTINUED FROM THE SECOND SHEET)

Category *	Citation of Document, ** with indication, where appropriate, of the relevant passages	Relevant to Claim No.
	(31.10.84), see abstract; page 1, line 1 - page 3, line 12; page 3, line 32 - page 5, line 22; fig. 1. --	
A	US, A, 4 853 962 (BROCKMANN) 01 August 1989 (01.08.89), see abstract; column 1, line 61 - column 2, line 2. --	1
A	Informationstechnik It, vol. 28, no. 3, 1986, Oldenbourg Verlag, DE, H. Sedlak "Ein Public-Key-Code Kryptographie-Prozessor", pages 157-161, see page 157, left-hand column, line 26 - right-hand column, line 32. ----	1

ANHANG
zum internationalen Recherchenbericht über die internationale Patentanmeldung Nr.

ANNEX
to the International Search Report to the International Patent Application No.

ANNEXE
au rapport de recherche international relatif á la demande de brevet international n°

PCT/GB91/00227 SAE 44571

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten internationalen Recherchenbericht angeführten Patentdokumente angegeben. Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

This Annex lists the patent family members relating to the patent documents cited in the above-mentioned international search report. The Office is in no way liable for these particulars which are given merely for the purpose of information.

La présente annexe indique les membres de la famille de brevets relatifs aux documents de brevets cités dans le rapport de recherche international visée ci-dessus. Les renseignements fournis sont donnés á titre indicatif et n'engagent pas la responsibilité de l'Office.

Im Recherchenbericht angeführtes Patentdokument Patent document cited in search report Document de brevet cité dans le rapport de recherche	Datum der Veröffentlichung Publication date Date de publication	Mitglied(er) der Patentfamilie Patent family member(s) Membre(s) de la famille de brevets	Datum der Veröffentlichung Publication date Date de publication
US-A - 4887296	12-12-89	CA-A1- 1244090	01-11-88
		EP-A2- 179612	30-04-86
		EP-A3- 179612	24-06-87
		JP-A2-61107376	26-05-86
		JP-B4- 2025186	31-05-90
EP-A1- 287720	26-10-88	JP-A2-63274242	11-11-88
		US-A - 4912762	27-03-90
EP-A1- 123360	31-10-84	CA-A1- 1220536	14-04-87
		DE-C0- 3462649	16-04-87
		EP-B1- 123360	11-03-87
		JP-A2-59207759	24-11-84
		NL-A - 8301458	16-11-84
		US-A - 4607137	19-08-86
EP-A1- 127381	05-12-84	AU-A1-28707/84	29-11-84
		AU-B2- 559463	12-03-87
		CA-A1- 1242793	04-10-88
		CA-A2- 1264848	23-01-90
		DE-C0- 3470368	11-05-88
		DK-A0- 2554/84	21-05-84
		DK-A - 2554/84	28-11-84
		EP-B1- 127381	06-04-88
		JP-A2-60057783	03-04-85
		JP-A2- 2096489	09-04-90
		NO-A - 842067	28-11-84
		NO-B - 166110	18-02-91
		US-A - 4613901	23-09-86
US-A - 4853962	01-08-89	Keine - None - Rien	